Mathematicians Will Never Stop to Provide New Proofs of the Infinitude of Primes

Hikmet Burak Özcan
(*joint work with Haydar Göral*)

İzmir Institute of Technology

İzmir Mathematics Days 3, Dokuz Eylül University

01 October 2020

The Book

- Paul Erdős has a theory that God has a book called "**The Book**"containing all the theorems of mathematics with their most beautiful proofs.

The Book

- Paul Erdős has a theory that God has a book called "**The Book**"containing all the theorems of mathematics with their most beautiful proofs.
- Erdős' this claim prompted many mathematicians to seek **new proofs** of theorems already proven.

The Book

- Paul Erdős has a theory that God has a book called "**The Book**"containing all the theorems of mathematics with their most beautiful proofs.
- Erdős' this claim prompted many mathematicians to seek **new proofs** of theorems already proven.
- In this talk, we will talk about new proofs of Euclid's theorem.

Euclid's Theorem

There are infinitely many prime numbers.

Euclid's Theorem

There are infinitely many prime numbers.

- The first proof of the infinitude of prime numbers is attributed to the ancient Greek mathematician Euclid.

Euclid's Theorem

There are infinitely many prime numbers.

- The first proof of the infinitude of prime numbers is attributed to the ancient Greek mathematician Euclid.
- He offered a proof published in his work "*Elements*"in 300 BC.

Euclid's Theorem

There are infinitely many prime numbers.

- The first proof of the infinitude of prime numbers is attributed to the ancient Greek mathematician Euclid.
- He offered a proof published in his work "*Elements*"in 300 BC.
- To prove the infinitude of primes, Euclid used the following fact:

Euclid's Theorem

There are infinitely many prime numbers.

- The first proof of the infinitude of prime numbers is attributed to the ancient Greek mathematician Euclid.
- He offered a proof published in his work "*Elements*"in 300 BC.
- To prove the infinitude of primes, Euclid used the following fact:

Every positive integer $n > 1$ **has a prime factor**.

Euclid's Proof

Suppose that $\mathbb{P} = \{p_1, \ldots, p_k\}$ is the set of all prime numbers.

Euclid's Proof

Suppose that $\mathbb{P} = \{p_1, \ldots, p_k\}$ is the set of all prime numbers. Let

$$n = p_1 \cdots p_k + 1.$$

Euclid's Proof

Suppose that $\mathbb{P} = \{p_1, \ldots, p_k\}$ is the set of all prime numbers. Let

$$n = p_1 \cdots p_k + 1.$$

As $n > 1$, it is divisible by a prime number $p \in \mathbb{P}$.

Euclid's Proof

Suppose that $\mathbb{P} = \{p_1, \ldots, p_k\}$ is the set of all prime numbers. Let

$$n = p_1 \cdots p_k + 1.$$

As $n > 1$, it is divisible by a prime number $p \in \mathbb{P}$. But, $p_1 \cdots p_k$ is also divisible by p, which implies that 1 is divisible by p.

Euclid's Proof

Suppose that $\mathbb{P} = \{p_1, \dots, p_k\}$ is the set of all prime numbers. Let

$$n = p_1 \cdots p_k + 1.$$

As $n > 1$, it is divisible by a prime number $p \in \mathbb{P}$. But, $p_1 \cdots p_k$ is also divisible by p, which implies that 1 is divisible by p. It is a contradiction. Thus, there are infinitely many prime numbers. $\square$

- After Euclid, new proofs are given to the infinitude of prime numbers using many different ways.

- After Euclid, new proofs are given to the infinitude of prime numbers using many different ways.

Euclidean Type Proofs:

- These proofs are based on the fact that every integer $n > 1$ has a prime divisor as in Euclid's proof, or the fundamental theorem of arithmetic.

- After Euclid, new proofs are given to the infinitude of prime numbers using many different ways.

Euclidean Type Proofs:

- These proofs are based on the fact that every integer $n > 1$ has a prime divisor as in Euclid's proof, or the fundamental theorem of arithmetic.

A Topological Proof:

- One of the most elegant proofs that prime numbers are infinite is Furstenberg's extraordinary proof using the basic concepts of topology.

- After Euclid, new proofs are given to the infinitude of prime numbers using many different ways.

Euclidean Type Proofs:

- These proofs are based on the fact that every integer $n > 1$ has a prime divisor as in Euclid's proof, or the fundamental theorem of arithmetic.

A Topological Proof:

- One of the most elegant proofs that prime numbers are infinite is Furstenberg's extraordinary proof using the basic concepts of topology.

Two Proofs by Additive Combinatorics:

- Using a deep result in additive combinatorics, van der Waerden's theorem, Alpoge and then Granville gave two subtle proofs of Euclid's theorem.

An Analytic Proof:

- Euler gave a proof of the infinitude of prime numbers using the fact the divergence of the harmonic series.

An Analytic Proof:

- Euler gave a proof of the infinitude of prime numbers using the fact the divergence of the harmonic series. He discovered an unexpected connection between prime numbers and infinite series:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1},$$

for any real number $s > 1$, where $\mathbb{P}$ is the set of all prime numbers.

An Analytic Proof:

- Euler gave a proof of the infinitude of prime numbers using the fact the divergence of the harmonic series. He discovered an unexpected connection between prime numbers and infinite series:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1},$$

  for any real number $s > 1$, where $\mathbb{P}$ is the set of all prime numbers.
- This discovery is considered as the beginning of the subject of analytic number theory.

- Apart from these, numerous new proofs have been given to the infinitude of prime numbers using many different ways such as arithmetic, combinatorics, dynamical systems, geometry, ring theory and so on.

- Apart from these, numerous new proofs have been given to the infinitude of prime numbers using many different ways such as arithmetic, combinatorics, dynamical systems, geometry, ring theory and so on.
- Meštrović collected 183 different proofs of Euclid's theorem with a nice historical perspective.

So Why?

- Why have mathematicians tried to prove the infinitude of prime numbers over and over again, although it has been known since 300 BC?

So Why?

- Why have mathematicians tried to prove the infinitude of prime numbers over and over again, although it has been known since 300 BC?

"*The theorem was never about the theorem. It was always about the proof.* "

-Micheal Bode-

The Contribution of A New Proof of Euclid's Theorem

- Euler's proof of the infinitude of prime numbers inspired Dirichlet. Combining the same idea with complex analysis he proved Dirichlet's Theorem on Arithmetic Progressions:

The Contribution of A New Proof of Euclid's Theorem

- Euler's proof of the infinitude of prime numbers inspired Dirichlet. Combining the same idea with complex analysis he proved Dirichlet's Theorem on Arithmetic Progressions:

Dirichlet's Theorem on Arithmetic Progressions

For any two positive coprime integers a and d, the arithmetic progression

$$a, a+d, a+2d, a+3d, \ldots$$

contains infinitely many prime numbers.

Three Short New Proofs

- Now, we will prensent our three new proofs of Euclid's theorem.

Three Short New Proofs

- Now, we will prensent our three new proofs of Euclid's theorem.
- The first will be Euclidean type proof.

Three Short New Proofs

- Now, we will prensent our three new proofs of Euclid's theorem.
- The first will be Euclidean type proof.
- The other two will be algebraic proofs. In fact, we will use a significant property of an object, the Jacobson radical, in ring theory.

Euclidean Type Proof

Proof [*Göral, Ö. (2020)*]

Euclidean Type Proof

Proof [*Göral, Ö. (2020)*]

Suppose that $p_1, \ldots, p_n$ is a complete list of all prime numbers.

Euclidean Type Proof

Proof [*Göral, Ö. (2020)*]

Suppose that $p_1, \ldots, p_n$ is a complete list of all prime numbers. Choose an arbitrary positive integer a and let $\mathcal{P} = p_1 \cdots p_n$.

Euclidean Type Proof

Proof [*Göral, Ö. (2020)*]

Suppose that $p_1, \ldots, p_n$ is a complete list of all prime numbers. Choose an arbitrary positive integer a and let $\mathcal{P} = p_1 \cdots p_n$. It is clear that $\mathcal{P} \neq 0$ and observe that the positive integer $a\mathcal{P}^2 + \mathcal{P}$ is divisible by all prime numbers $p_1, \ldots, p_n$.

Euclidean Type Proof

Proof [*Göral, Ö. (2020)*]

Suppose that $p_1, \dots, p_n$ is a complete list of all prime numbers. Choose an arbitrary positive integer a and let $\mathcal{P} = p_1 \cdots p_n$. It is clear that $\mathcal{P} \neq 0$ and observe that the positive integer $a\mathcal{P}^2 + \mathcal{P}$ is divisible by all prime numbers $p_1, \dots, p_n$. But, p^2 does not divide $a\mathcal{P}^2 + \mathcal{P}$ for any $p \in \{p_1, \dots, p_n\}$.

Euclidean Type Proof

Proof [*Göral, Ö. (2020)*]

Suppose that $p_1, \ldots, p_n$ is a complete list of all prime numbers. Choose an arbitrary positive integer a and let $\mathcal{P} = p_1 \cdots p_n$. It is clear that $\mathcal{P} \neq 0$ and observe that the positive integer $a\mathcal{P}^2 + \mathcal{P}$ is divisible by all prime numbers $p_1, \ldots, p_n$. But, p^2 does not divide $a\mathcal{P}^2 + \mathcal{P}$ for any $p \in \{p_1, \ldots, p_n\}$. By Fundamental Theorem of Arithmetic, we obtain that

$$a\mathcal{P}^2 + \mathcal{P} = \mathcal{P}.$$

Euclidean Type Proof

Proof [*Göral, Ö. (2020)*]

Suppose that $p_1, \dots, p_n$ is a complete list of all prime numbers. Choose an arbitrary positive integer a and let $\mathcal{P} = p_1 \cdots p_n$. It is clear that $\mathcal{P} \neq 0$ and observe that the positive integer $a\mathcal{P}^2 + \mathcal{P}$ is divisible by all prime numbers $p_1, \dots, p_n$. But, p^2 does not divide $a\mathcal{P}^2 + \mathcal{P}$ for any $p \in \{p_1, \dots, p_n\}$. By Fundamental Theorem of Arithmetic, we obtain that

$$a\mathcal{P}^2 + \mathcal{P} = \mathcal{P}.$$

This gives that $a = 0$. In other words, all positive integers are equal to 0, which is absurd. $\square$

Two Proofs by Ring Theory

Two Proofs by Ring Theory

Definition

The *Jacobson radical* $J(R)$ of a commutative ring R is the intersection of all maximal ideals of R.

Two Proofs by Ring Theory

Definition

The *Jacobson radical* $J(R)$ of a commutative ring R is the intersection of all maximal ideals of R.

- Using the following property of the Jacobson radical, we will give two new proofs of Euclid's theorem.

Two Proofs by Ring Theory

Definition

The *Jacobson radical* $J(R)$ of a commutative ring R is the intersection of all maximal ideals of R.

- Using the following property of the Jacobson radical, we will give two new proofs of Euclid's theorem.

Lemma

For any commutative ring R, we have

1. $1 - x$ *is a unit for each* $x \in J(R)$.
2. *The Jacobson radical is the largest ideal such that* $1 - x$ *is a unit for each* $x \in J(R)$.

Two Proofs by Ring Theory

Proof 1 [*Göral, Ö. (2020)*]

Two Proofs by Ring Theory

Proof 1 [*Göral, Ö. (2020)*]

Suppose that $p_1, \ldots, p_n$ are all prime numbers, where $p_1 = 2$.

Two Proofs by Ring Theory

Proof 1 [*Göral, Ö. (2020)*]

Suppose that $p_1, \ldots, p_n$ are all prime numbers, where $p_1 = 2$. Then, $p_i\mathbb{Z} \subset \mathbb{Z}$ is a maximal ideal for evey $i = 1, \ldots, n$. In fact, these are all maximal ideals in $\mathbb{Z}$.

Two Proofs by Ring Theory

Proof 1 [*Göral, Ö. (2020)*]

Suppose that $p_1, \ldots, p_n$ are all prime numbers, where $p_1 = 2$. Then, $p_i\mathbb{Z} \subset \mathbb{Z}$ is a maximal ideal for evey $i = 1, \ldots, n$. In fact, these are all maximal ideals in $\mathbb{Z}$. Hence,

$$J(\mathbb{Z}) = \bigcap_{i=1}^{n} p_i\mathbb{Z} = (p_1 \cdots p_n)\mathbb{Z}.$$

Two Proofs by Ring Theory

Proof 1 [*Göral, Ö. (2020)*]

Suppose that $p_1, \ldots, p_n$ are all prime numbers, where $p_1 = 2$. Then, $p_i\mathbb{Z} \subset \mathbb{Z}$ is a maximal ideal for evey $i = 1, \ldots, n$. In fact, these are all maximal ideals in $\mathbb{Z}$. Hence,

$$J(\mathbb{Z}) = \bigcap_{i=1}^{n} p_i\mathbb{Z} = (p_1 \cdots p_n)\mathbb{Z}.$$

Observe that $p_1 \cdots p_n \in J(\mathbb{Z})$.

Two Proofs by Ring Theory

Proof 1 [*Göral, Ö. (2020)*]

Suppose that $p_1, \ldots, p_n$ are all prime numbers, where $p_1 = 2$. Then, $p_i\mathbb{Z} \subset \mathbb{Z}$ is a maximal ideal for evey $i = 1, \ldots, n$. In fact, these are all maximal ideals in $\mathbb{Z}$. Hence,

$$J(\mathbb{Z}) = \bigcap_{i=1}^{n} p_i\mathbb{Z} = (p_1 \cdots p_n)\mathbb{Z}.$$

Observe that $p_1 \cdots p_n \in J(\mathbb{Z})$. By Lemma, $1 - p_1 \cdots p_n$ is a unit.

Two Proofs by Ring Theory

Proof 1 [*Göral, Ö. (2020)*]

Suppose that $p_1, \ldots, p_n$ are all prime numbers, where $p_1 = 2$. Then, $p_i\mathbb{Z} \subset \mathbb{Z}$ is a maximal ideal for evey $i = 1, \ldots, n$. In fact, these are all maximal ideals in $\mathbb{Z}$. Hence,

$$J(\mathbb{Z}) = \bigcap_{i=1}^{n} p_i\mathbb{Z} = (p_1 \cdots p_n)\mathbb{Z}.$$

Observe that $p_1 \cdots p_n \in J(\mathbb{Z})$. By Lemma, $1 - p_1 \cdots p_n$ is a unit. Since, $p_1 \cdots p_n > 1$, we deduce that

$$1 - p_1 \cdots p_n = -1.$$

Two Proofs by Ring Theory

Proof 1 [*Göral, Ö. (2020)*]

Suppose that $p_1, \ldots, p_n$ are all prime numbers, where $p_1 = 2$. Then, $p_i\mathbb{Z} \subset \mathbb{Z}$ is a maximal ideal for evey $i = 1, \ldots, n$. In fact, these are all maximal ideals in $\mathbb{Z}$. Hence,

$$J(\mathbb{Z}) = \bigcap_{i=1}^{n} p_i\mathbb{Z} = (p_1 \cdots p_n)\mathbb{Z}.$$

Observe that $p_1 \cdots p_n \in J(\mathbb{Z})$. By Lemma, $1 - p_1 \cdots p_n$ is a unit. Since, $p_1 \cdots p_n > 1$, we deduce that

$$1 - p_1 \cdots p_n = -1.$$

So, $p_1 \cdots p_n = 2$ which means that 2 is the only prime number. $\square$

Two Proofs by Ring Theory

Proof 2 [*Göral, Ö. (2020)*]

Two Proofs by Ring Theory

Proof 2 [*Göral, Ö. (2020)*]

Let $x \in J(\mathbb{Z})$ be arbitrary.

Two Proofs by Ring Theory

Proof 2 [*Göral, Ö. (2020)*]

Let $x \in J(\mathbb{Z})$ be arbitrary. Since $J(\mathbb{Z})$ is an ideal, $-x \in J(\mathbb{Z})$.

Two Proofs by Ring Theory

Proof 2 [*Göral, Ö. (2020)*]

Let $x \in J(\mathbb{Z})$ be arbitrary. Since $J(\mathbb{Z})$ is an ideal, $-x \in J(\mathbb{Z})$. By Lemma, both $1 - x$ and $1 + x$ are units of $\mathbb{Z}$.

Two Proofs by Ring Theory

Proof 2 [*Göral, Ö. (2020)*]

Let $x \in J(\mathbb{Z})$ be arbitrary. Since $J(\mathbb{Z})$ is an ideal, $-x \in J(\mathbb{Z})$. By Lemma, both $1 - x$ and $1 + x$ are units of $\mathbb{Z}$. In other words, $1 - x$ and $1 + x$ belong to $\{-1, 1\}$.

Two Proofs by Ring Theory

Proof 2 [*Göral, Ö. (2020)*]

Let $x \in J(\mathbb{Z})$ be arbitrary. Since $J(\mathbb{Z})$ is an ideal, $-x \in J(\mathbb{Z})$. By Lemma, both $1 - x$ and $1 + x$ are units of $\mathbb{Z}$. In other words, $1 - x$ and $1 + x$ belong to $\{-1, 1\}$. This in only possible when $x = 0$.

Two Proofs by Ring Theory

Proof 2 [*Göral, Ö. (2020)*]

Let $x \in J(\mathbb{Z})$ be arbitrary. Since $J(\mathbb{Z})$ is an ideal, $-x \in J(\mathbb{Z})$. By Lemma, both $1-x$ and $1+x$ are units of $\mathbb{Z}$. In other words, $1-x$ and $1+x$ belong to $\{-1,1\}$. This in only possible when $x=0$. Thus, $J(\mathbb{Z})=\{0\}$.

Two Proofs by Ring Theory

Proof 2 [*Göral, Ö. (2020)*]

Let $x \in J(\mathbb{Z})$ be arbitrary. Since $J(\mathbb{Z})$ is an ideal, $-x \in J(\mathbb{Z})$. By Lemma, both $1 - x$ and $1 + x$ are units of $\mathbb{Z}$. In other words, $1 - x$ and $1 + x$ belong to $\{-1, 1\}$. This in only possible when $x = 0$. Thus, $J(\mathbb{Z}) = \{0\}$. However, we know that

$$J(\mathbb{Z}) = \bigcap_{p \in \mathbb{P}} p\mathbb{Z},$$

where $\mathbb{P}$ is the set of all prime numbers.

Two Proofs by Ring Theory

Proof 2 [*Göral, Ö. (2020)*]

Let $x \in J(\mathbb{Z})$ be arbitrary. Since $J(\mathbb{Z})$ is an ideal, $-x \in J(\mathbb{Z})$. By Lemma, both $1-x$ and $1+x$ are units of $\mathbb{Z}$. In other words, $1-x$ and $1+x$ belong to $\{-1,1\}$. This in only possible when $x=0$. Thus, $J(\mathbb{Z})=\{0\}$. However, we know that

$$J(\mathbb{Z}) = \bigcap_{p \in \mathbb{P}} p\mathbb{Z},$$

where $\mathbb{P}$ is the set of all prime numbers. If there were finitely many prime numbers $p_1, \ldots, p_n$, then $J(\mathbb{Z})$ would contain a non-zero product $p_1 \cdots p_n$.

Two Proofs by Ring Theory

Proof 2 [*Göral, Ö. (2020)*]

Let $x \in J(\mathbb{Z})$ be arbitrary. Since $J(\mathbb{Z})$ is an ideal, $-x \in J(\mathbb{Z})$. By Lemma, both $1-x$ and $1+x$ are units of $\mathbb{Z}$. In other words, $1-x$ and $1+x$ belong to $\{-1,1\}$. This in only possible when $x=0$. Thus, $J(\mathbb{Z}) = \{0\}$. However, we know that

$$J(\mathbb{Z}) = \bigcap_{p \in \mathbb{P}} p\mathbb{Z},$$

where $\mathbb{P}$ is the set of all prime numbers. If there were finitely many prime numbers $p_1, \ldots, p_n$, then $J(\mathbb{Z})$ would contain a non-zero product $p_1 \cdots p_n$. Therefore, there must be infinitely many prime numbers. $\square$

References

- L. Alpoge, *Van der Waerden and the Primes*, The American Mathematical Monthly **122** (2015), no. 8, 784-785.
- P. Erdős, *Uber die Reihe* $\sum \frac{1}{p}$, Mathematica (Zutphen), B7 (1938) 1-2.
- L. Euler, *Variae observationes circa series infinitas*, Com. Acad. Scient. Petropl., **9** (1744), 160–188. Online at https://scholarlycommons.pacific.edu/euler-works.
- H. Furstenberg, *On the infinitude of primes*, American Mathematical Monthly, **62** (1955), 353.
- H. Göral, H. B. Özcan *Several Novel Proofs of the Infinitude of Primes*, The Mathematics Student, **89** (2020).
- R. Meštrović, Euclid's theorem on the infinitude of primes: A historical survey of its proofs, https://arxiv.org/pdf/1202.3670.pdf

THANK YOU

Loading new proofs... :)